GOVERNMENT INFORMATION STEWARDSHIP ACT

GISA

Deep research report, comparative-law analysis, and model federal statute

A technology-neutral legal framework for the creation, acquisition, provenance, jurisdiction, movement, transformation, use, retention, and destruction of government-held information about identifiable persons.

Prepared as a standalone legislative proposal drawing on the Private Infrastructure, Public Power problem brief, the first-generation lifecycle report, the comparative data-sovereignty supplement, and additional primary-source research.

Research current through July 19, 2026. This report is policy research and model legislation, not legal advice.

Executive Summary

Government increasingly acquires information through sensors, commercial databases, cloud platforms, body-worn cameras, license-plate networks, facial-recognition services, communications providers, and AI systems. Existing American law regulates fragments of this environment: the Fourth Amendment governs some acquisitions and searches; the Privacy Act governs some federal systems of records; the Federal Records Act governs preservation and disposition; the Stored Communications Act governs specified provider disclosures; criminal-history regulations govern dissemination; and security standards protect certain systems. No general statute defines the obligations that attach to government information throughout its legal existence.

GISA supplies that missing framework. Its governing concept is stewardship. A governmental entity that creates, acquires, controls, licenses, queries, or materially relies upon identifiable information becomes responsible for its provenance, legal authority, accuracy, custody, movement, transformation, use, descendants, retention, and destruction. Outsourcing does not extinguish that responsibility.

The Act is built around operations rather than technologies. Collection, acquisition, validation, consultation, querying, alteration, combination, inference, replication, transfer, disclosure, training use, archival preservation, and deletion are separate stewardship events. Each event requires authority, metadata, access control, logging, and a purpose compatible with the record's governing restrictions.

Comparative law supports this architecture. The European Union Law Enforcement Directive separately regulates and requires logging of collection, alteration, consultation, disclosure, transfers, combination, and erasure. Brazil's LGPD defines processing through a similarly granular list of verbs. Russia makes physical database location independently legally significant. China combines localization for higher-risk data with transfer gates. Australia and Canada preserve the originating entity's accountability after outsourcing and overseas processing. GISA adapts the useful mechanisms while rejecting blanket localization and authoritarian control models.

Domestic analogues reinforce the proposal. NARA's electronic-records requirements organize obligations around capture, maintenance and use, disposal, transfer, metadata, and reporting. Criminal-history regulations limit dissemination by purpose and provide access and correction rights. CJIS policy requires auditability and security across public and private handlers. HIPAA uses role-based safeguards, access rights, business-associate responsibility, and audit controls. Classified-information rules require markings, derivative-classification lineage, dissemination controls, and declassification review. NIST AI guidance emphasizes inventories, provenance, data lineage, model documentation, and audit trails. GISA synthesizes these mature mechanisms into a general public-law code.

Principal innovations:

- Every covered record has an origin, legal authority, primary jurisdiction, purpose, sensitivity tier, confidence status, and authoritative copy.
- Every material transformation creates a separately governed derived record linked to its source records and the model, method, and version that produced it.
- Restrictions follow the record and ordinarily flow to replicas, recipients, indexes, embeddings, transcripts, association graphs, and other identifiable descendants.
- Remote access, replication, interagency querying, foreign administration, bulk export, and onward transfer are separate legal events even when no file is visibly downloaded.
- Government remains accountable after outsourcing and cannot disclaim responsibility merely because a contractor or another jurisdiction processes the information.
- AI training and cross-agency model development require express authority, segregated datasets, version control, impact assessment, and independent oversight.
- Retention requires both a maximum period and periodic necessity review; deletion must address reasonably identifiable descendants, not merely the source file.

- Individuals receive calibrated rights to notice, access, correction, provenance, explanation, and challenge when information materially contributes to adverse governmental action.

1. Problem Definition and Continuity

The project's original problem brief documented a recurring public-private pipeline: collection by a private or public sensor; aggregation by a vendor; government access; algorithmic inference; coercive action; and a final accountability gap in which each actor points to another. GISA addresses the information after it enters governmental control or materially influences governmental action. The companion Public Power Through Private Infrastructure Act regulates the market that supplies the capability.

Observed failure	Why current law is incomplete	GISA response
Government data is copied across clouds and jurisdictions	Records, privacy, security, evidence, and procurement rules operate in separate silos	Treat replication, remote access, export, and onward transfer as logged legal events
AI converts observations into identities, graphs, and risk assessments	Current rules rarely define derivative information or inherited restrictions	Create derived-record status, lineage metadata, model-version records, and corroboration duties
Data retained for one purpose is reused for another	Purpose rules vary by statute and are often database-specific	Attach machine-readable purpose and compatibility restrictions to the record
A source file is deleted while indexes and inferences remain	Deletion rules often focus on the named record or system	Require descendant identification and deletion or independent legal authority
Contractors hold operational control	Agency responsibility can become practically diffuse	Impose nondelegable stewardship duties and contractor flow-down clauses
A citizen cannot identify or correct the data behind an adverse action	Access rights depend on sector, record system, and exemption	Create calibrated notice, provenance, correction, and contest rights

2. Existing United States Law: Strong Modules, No General Code

2.1 Fourth Amendment doctrine

United States v. Jones, Riley v. California, Carpenter v. United States, and Chatrie v. United States establish that digital scale, persistence, aggregation, and reverse identification can matter constitutionally. Those decisions constrain particular government searches; they do not provide a comprehensive stewardship code governing every subsequent copy, transformation, transfer, model use, or deletion decision. GISA operates above the constitutional floor and does not purport to redefine what is a search.

2.2 Privacy Act of 1974

The Privacy Act, 5 U.S.C. § 552a, provides a partial architecture: system notices, accuracy and relevance duties, access and amendment, disclosure accounting, purpose constraints, and contractor provisions. Its limits are equally instructive. It is federal, turns on systems of records and retrieval by personal identifier, contains broad exemptions, and was not designed for shared cloud platforms, graph databases, probabilistic inferences, embeddings, or cross-jurisdiction vendor networks.

2.3 Federal Records Act and NARA

The Federal Records Act and NARA regulations govern creation, maintenance, transfer, and authorized disposition of federal records. NARA's Universal Electronic Records Management Requirements expressly organize electronic-record management around capture, maintenance and use, disposal, transfer, metadata, and reporting. NARA also requires metadata sufficient to identify, service, interpret, preserve, and protect transferred electronic records. These rules validate a lifecycle architecture but primarily protect governmental evidence and historical accountability, not all individual rights or operational surveillance uses.

2.4 Criminal history information

28 C.F.R. part 20 applies to state and local systems collecting, storing, or disseminating criminal-history record information and to federal exchange systems. It limits noncriminal-justice use to the purpose for which information was given, requires procedures for dissemination, and provides an individual access and challenge mechanism. This is a direct domestic precedent for purpose limitation, controlled dissemination, and correction in government information systems.

2.5 CJIS Security Policy

The FBI CJIS Security Policy supplies detailed security, authentication, audit, media, incident-response, and contractor controls. It demonstrates that government can impose common handling requirements across federal, state, local, tribal, and private entities that access criminal justice information. GISA borrows the compliance architecture but adds substantive limits on purpose, transformation, movement, and retention.

2.6 Stored Communications Act and commercial acquisition

The Stored Communications Act regulates specified disclosures by electronic communications and remote computing service providers. Its category-based process rules do not reach every commercial dataset or remote query. GISA therefore adopts legal-process parity: government may not use purchase, licensing, API access, a trial account, or a private intermediary to obtain materially equivalent information with less process than direct compulsion would require.

2.7 Sectoral analogues: HIPAA, FCRA, DPPA, classified information

Regime	Mechanism worth borrowing	GISA adaptation
HIPAA Privacy and Security Rules	Minimum-necessary use, individual access/amendment, business-associate responsibility, audit controls	Purpose-limited government use, contractor responsibility, access logs, correction
FCRA	Permissible purposes, accuracy, dispute/reinvestigation, user duties, civil remedies	Accuracy and dispute rights when data contributes to adverse governmental action
DPPA	Default nondisclosure, enumerated permissible uses, redisclosure controls	Enumerated movement/use authority and restrictions that bind recipients
Classified-information system	Markings, derivative classification, dissemination controls, training, declassification review	Machine-readable restrictions, derived-record inheritance, trained stewards, periodic declassification/deletion review
NIST AI RMF and GenAI Profile	Inventories, provenance, lineage, model documentation, testing, version control	AI system inventory, model/version provenance, lineage, TEVV and audit trails

3. Comparative Law

3.1 European Union Law Enforcement Directive

Directive (EU) 2016/680 is the closest enacted analogue. It regulates personal-data processing by competent authorities for criminal-law and public-security purposes. Articles 4 and 5 impose purpose limitation, minimization, accuracy, security, and review or erasure deadlines. Article 9 regulates new-purpose processing. Article 25 requires logs for collection, alteration, consultation, disclosure including transfers, combination, and erasure, sufficient to establish justification, timing, user, and recipient. Its transfer provisions preserve controls over onward transfers. GISA adopts this operation-level conception while adapting it to U.S. constitutional structure.

3.2 Brazil

Brazil's LGPD defines processing through an unusually comprehensive list: collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, deletion,

evaluation, modification, communication, transfer, diffusion, and extraction. That drafting choice strongly supports GISA's verb-based scope. Brazil also regulates public-sector sharing and international transfers.

3.3 Russia

Russian Federal Law No. 242-FZ requires specified operations involving Russian citizens' personal data to use databases located in the Russian Federation. The useful lesson is narrow: physical location and an authoritative domestic database can be independent legal variables. GISA rejects blanket localization and the Russian enforcement model, but adopts transparent storage-location inventories and limited domestic-residency requirements for the highest-risk federal information.

3.4 China

China's Personal Information Protection Law combines domestic storage for specified high-risk operators with security assessments, certifications, standard contracts, and separate consent for many cross-border transfers. The transferable mechanism is tiering: high-risk data and processors receive stronger residency and export controls. GISA uses risk tiers and transfer authorization, not broad state control or consent fiction in the law-enforcement context.

3.5 Australia and Canada

Australia and Canada generally rely on accountability rather than categorical localization. The originating entity remains responsible for protective arrangements when data is processed by an overseas recipient or service provider. GISA adopts the same anti-laundering principle: legal custody and responsibility survive outsourcing, replication, and interjurisdictional processing.

Comparative mechanism	Adopt?	GISA treatment
Operation-level logging	Yes	Mandatory logs for acquisition, consultation, alteration, inference, transfer, training, and deletion
Periodic erasure/review deadlines	Yes	Maximum retention plus recurring necessity review
Origin approval for onward transfer	Yes	Primary steward approval with emergency override and later review
Blanket citizen-data localization	No	Too rigid; risks fragmentation and false security
Tiered domestic residency	Limited	Highest-risk federal data; exceptions for equivalent protection and resilience
Exporter/originator accountability	Yes	Nondelegable stewardship after outsourcing
Processing defined by verbs	Yes	Technology-neutral lifecycle operations definition

4. General Theory of Government Information Stewardship

Authority attaches at creation or acquisition

A record cannot lawfully enter a covered system without an identified authority, purpose, source category, and responsible steward.

Provenance is a legal attribute

Origin, collector, time, method, authority, confidence, and modifications are part of the legal record, not optional technical metadata.

Movement is a legal event

Replication, remote access, API querying, bulk export, and onward disclosure must be authorized and logged.

Transformation creates a derived record

OCR, face matching, entity resolution, transcription, association analysis, risk scoring, and model output create separately governed objects.

Restrictions follow the record

Purpose, jurisdiction, sensitivity, and retention constraints propagate to copies and derivatives unless a statute clearly authorizes otherwise.

Government cannot outsource accountability

The steward remains responsible for contractors, cloud providers, subprocessors, and recipients.

Inference is weaker than observation

Probabilistic or model-derived outputs require confidence disclosure, corroboration, and preservation of source and version information.

Retention requires justification

Cheap storage and hypothetical future usefulness are not sufficient.

Deletion is graph-aware

The duty reaches identifiable copies and descendants, with transparent exceptions for archival law, litigation holds, and technically inseparable model weights.

Every stewardship operation is auditable

A system that cannot reconstruct who did what, when, why, under what authority, and with what downstream effect is unfit for covered use.

5. Risk Tiers

GISA should calibrate duties to sensitivity and consequence rather than impose identical controls on every government record.

Tier	Illustrative data	Core controls
Tier 1 - Administrative	Routine contact and service records with limited coercive use	Baseline security, purpose, retention, access accounting
Tier 2 - Investigative	Body-camera evidence, ALPR records, case files, communications metadata	Enhanced access, provenance, dissemination controls, correction and notice after action
Tier 3 - Sensitive	Biometrics, precise location, health, religious/political association, minors, domestic-violence shelter data	Judicial/process thresholds, strict sharing, short default retention, domestic primary copy
Tier 4 - Derived high-impact	Risk scores, watchlists, identity graphs, predictive inferences, AI-generated investigative leads	Model/version lineage, independent validation, human review, corroboration, appeal
Tier 5 - Restricted systemic	Bulk nationwide datasets, cross-agency training corpora, persistent population-scale tracking	Express statutory authorization, independent board approval, public findings, continuous audit

6. Model Federal Statute

The following draft is a model for legislative counsel. It separates current-law description from proposed policy and should be refined through hearings, federalism review, and technical consultation.

A BILL

To establish stewardship duties for government-held information relating to identifiable persons; to regulate the creation, acquisition, provenance, movement, transformation, use, retention, and destruction of such information; and for other purposes.

SECTION 1. SHORT TITLE.

This Act may be cited as the "Government Information Stewardship Act" or "GISA."

SEC. 2. FINDINGS.

Congress finds that—

(1) governmental entities increasingly create, acquire, license, query, and rely upon information maintained in distributed public and private systems;

(2) digital information may be replicated, remotely accessed, combined, inferred from, and transferred across jurisdictions without the visible movement associated with physical evidence;

(3) existing Federal law regulates portions of collection, records management, communications access, criminal-history dissemination, security, and privacy but does not establish a comprehensive stewardship code;

(4) operation-level logging, provenance, origin control, periodic review, and accountable outsourcing are established mechanisms in domestic and comparative law;

(5) AI and algorithmic systems create derived records that may materially influence governmental action and require source, model, version, confidence, and validation documentation; and

(6) uniform minimum standards are necessary to protect constitutional interests, individual rights, public safety, reliable evidence, federalism, and public trust.

SEC. 3. PURPOSES.

The purposes are to—

(1) establish nondelegable stewardship duties;

(2) treat material lifecycle operations as separately authorized and auditable events;

(3) preserve provenance, integrity, and jurisdictional control;

(4) regulate derived and AI-generated information;

(5) prevent legal-process and accountability circumvention;

(6) provide calibrated individual rights and remedies; and

(7) preserve stronger State protections.

SEC. 4. DEFINITIONS.

In this Act: "covered information" means information about an identified or reasonably identifiable natural person that is created, acquired, controlled, licensed, queried, or materially relied upon by a governmental entity. "Steward" means the governmental entity with primary legal responsibility. "Lifecycle operation" means collection, production, receipt, acquisition, ingestion, classification, validation, consultation, querying, reproduction, replication, alteration, combination, enrichment, inference, transmission, disclosure, transfer, export, archiving, storage, training use, deletion, destruction, or extraction. "Derived record" means information materially produced from one or more source records by human or automated transformation. "Authoritative copy" means the legally controlling record designated by the steward. "Material adverse governmental action"

includes arrest, detention, search, seizure, immigration action, watchlisting, denial of a benefit, or another action materially affecting liberty, property, or legal status.

SEC. 5. SCOPE AND EXCLUSIONS.

This Act applies to Federal entities and contractors and to recipients of designated Federal information-technology or law-enforcement funds. It does not apply to purely statistical information that cannot reasonably be linked to a person, personal notes not used for agency business, or information governed exclusively by a more protective classified-information regime, except that provenance and inspector-general access shall remain.

SEC. 6. DESIGNATION OF STEWARD.

Each covered system and dataset shall identify a steward, responsible official, primary legal jurisdiction, authoritative copy, purpose, risk tier, and governing authorities. Responsibility may not be disclaimed through contract or transfer.

SEC. 7. LAWFUL CREATION AND ACQUISITION.

Covered information may be created or acquired only under identified constitutional, statutory, regulatory, judicial, or consensual authority. The record shall include authority, purpose, source, collection method, date, jurisdiction, and reliability status. Commercial purchase or remote access may not be used to obtain materially equivalent information with less legal process than direct compulsion would require.

SEC. 8. DATA MINIMIZATION AND RELEVANCE.

A steward shall collect and retain only information reasonably necessary and proportionate to the authorized purpose, with special limits for sensitive locations, protected activity, minors, health, biometrics, and precise location.

SEC. 9. PROVENANCE METADATA.

Every covered record shall maintain machine-readable provenance sufficient to identify source, authority, time, collector or system, transformations, confidence, restrictions, copies, recipients, and disposition status. Removal or falsification of material provenance is prohibited.

SEC. 10. VALIDATION AND QUALITY STATUS.

Information shall be marked as verified fact, unverified allegation, estimate, automated match, human assessment, or other category prescribed by rule. Agencies shall distinguish source facts from assessments and correct material inaccuracies.

SEC. 11. AUTHORITATIVE COPY AND STORAGE INVENTORY.

Each system shall designate an authoritative copy and maintain an inventory of storage regions, legal jurisdictions, replicas, backups, caches, subprocessors, and remote-administration locations.

SEC. 12. RESIDENCY OF HIGH-RISK INFORMATION.

Tier 5 information and categories designated by Congress shall maintain an authoritative copy in the United States in an approved environment. The Attorney General may approve an exception upon findings of operational necessity, equivalent legal protection, cybersecurity, resilience, and oversight access.

SEC. 13. ACCESS CONTROL.

Access shall be role-based, purpose-limited, authenticated, periodically reviewed, and automatically suspended when authority ends. Shared accounts designed to defeat attribution are prohibited.

SEC. 14. OPERATION-LEVEL LOGGING.

Automated systems shall log acquisition, consultation, querying, alteration, combination, inference, disclosure, transfer, export, training use, and deletion. Logs shall identify justification, date and time, user or system, records affected, recipient, and authority.

SEC. 15. REPLICATION AND BACKUP.

Replication and backup require documented purpose, location, protection, restoration testing, and synchronized retention. A backup may not become an ungoverned archive or independent source of secondary use.

SEC. 16. INTERAGENCY QUERYING.

Remote query by another agency is a disclosure and consultation event. It requires an agreement specifying purpose, authority, user eligibility, redisclosure, audit access, correction propagation, and termination.

SEC. 17. CROSS-JURISDICTION AND INTERNATIONAL TRANSFER.

A transfer outside the primary jurisdiction requires documented authority, recipient safeguards, purpose compatibility, and steward approval. Onward transfer requires renewed approval unless an emergency exists. Origin restrictions bind recipients.

SEC. 18. CONTRACTORS AND SUBPROCESSORS.

Contracts shall impose equivalent duties, audit access, incident reporting, storage-location disclosure, subprocessor approval, deletion certification, portability, and termination assistance. The steward remains responsible for reasonable oversight.

SEC. 19. PURPOSE COMPATIBILITY.

Secondary use requires express authority or a written compatibility determination considering the original purpose, context, sensitivity, consequences, safeguards, and reasonable expectations. General intelligence value or technical feasibility alone is insufficient.

SEC. 20. MATERIAL TRANSFORMATION AND DERIVED RECORDS.

A material transformation creates a derived record with a new identifier, purpose, creator, method, time, confidence, and retention rule. The derived record shall remain linked to source records and inherit the most protective applicable restrictions absent express statutory authority.

SEC. 21. ALGORITHMIC AND AI USE.

A governmental entity shall maintain an inventory of covered models and systems; document training sources, versions, validation, limitations, and intended use; preserve outputs relied upon; and conduct predeployment and periodic impact assessments.

SEC. 22. AI TRAINING.

Covered information may not be used to train, fine-tune, benchmark, or validate a general-purpose or cross-agency model absent express authority, a segregated and versioned dataset, impact assessment, independent approval, and a specific retention and deletion schedule.

SEC. 23. CORROBORATION.

No material adverse governmental action may be based solely on an automated match, predictive score, association inference, or model-derived record. A trained official shall document independent corroboration and meaningful review.

SEC. 24. RETENTION SCHEDULES.

Each category shall have a maximum retention period and periodic necessity-review deadline. Storage cost, speculative future usefulness, or vendor default is not sufficient justification.

SEC. 25. HOLDS AND ARCHIVAL PRESERVATION.

Litigation, investigation, audit, public-records, and archival holds shall be documented, scoped, periodically reviewed, and released when no longer necessary. Archival preservation shall not authorize unrestricted operational querying.

SEC. 26. DELETION AND DESCENDANTS.

Upon deletion, the steward shall delete or render inaccessible reasonably identifiable replicas, indexes, caches, embeddings, transcripts, and derived records lacking independent authority. Technical inability to remove information from trained model weights shall be documented and shall trigger use restrictions and prohibition on further training from the source dataset.

SEC. 27. NOTICE OF MATERIAL RELIANCE.

When covered information materially contributes to a material adverse governmental action, the person shall receive notice of the information category, source category, and automated processing, subject to court-authorized delay.

SEC. 28. ACCESS AND PROVENANCE RIGHTS.

After lawful delay expires, a person may obtain covered information materially relied upon, relevant provenance, an accounting of queries and disclosures, and a description of material transformations, subject to protective orders and specified exemptions.

SEC. 29. CORRECTION AND REINVESTIGATION.

A person may dispute inaccurate, incomplete, misleading, or unverifiable information. The steward shall conduct a reasonable reinvestigation, annotate or correct the record, and propagate correction to material recipients and descendants.

SEC. 30. EXPLANATION AND CONTEST OF DERIVED RECORDS.

A person affected by a derived high-impact record may obtain a meaningful description of inputs, method, confidence, limitations, human review, and corroboration and may seek independent review.

SEC. 31. TRANSPARENCY REPORTING.

Agencies shall report system inventories, risk tiers, retention schedules, interagency and international transfers, AI uses, correction outcomes, incidents, exemptions, and compliance audits, with lawful redactions.

SEC. 32. INDEPENDENT OVERSIGHT BOARD.

An independent Government Information Stewardship Board shall issue guidance, approve Tier 5 systems, receive complaints, coordinate audits, and report to Congress. Members shall include legal, technical, civil-rights, records, security, and state/local expertise.

SEC. 33. INSPECTOR GENERAL AND AUDIT ACCESS.

Inspectors general and designated auditors shall have access to systems, contracts, logs, models, training documentation, and contractor facilities necessary to determine compliance.

SEC. 34. SECURITY AND INCIDENT RESPONSE.

NIST shall publish minimum security controls. Material incidents shall be contained, preserved, investigated, reported, and remediated. Affected persons shall be notified when risk warrants, subject to lawful delay.

SEC. 35. FEDERAL PROCUREMENT.

The FAR Council shall issue mandatory clauses implementing GISA, including flow-down, audit, data portability, location disclosure, deletion certification, model documentation, and suspension or debarment for material repeated violations.

SEC. 36. FEDERAL GRANT CONDITIONS.

Specified grants shall require prospective compliance by recipient agencies, clear notice, technical assistance, and reasonable implementation periods.

SEC. 37. ENFORCEMENT.

The Attorney General may seek declaratory, injunctive, and civil relief. Agency inspectors general may issue corrective recommendations. State attorneys general may enforce applicable grant and vendor provisions. Contractor violations may constitute false certification or grounds for suspension, debarment, and recovery.

SEC. 38. PRIVATE CIVIL ACTION.

A person materially harmed by a knowing or reckless violation of sections governing unlawful acquisition, prohibited use, falsified provenance, unauthorized transfer, automated adverse action, notice, access, or correction may seek actual damages, equitable relief, statutory damages for material violations, and reasonable attorney's fees, subject to carefully specified sovereign-immunity rules.

SEC. 39. EMERGENCIES.

Emergency action is permitted when reasonably necessary to prevent imminent death or serious bodily injury. The official shall document facts, scope, users, data accessed, and results and obtain judicial or supervisory review within 48 hours where process would otherwise be required.

SEC. 40. NATIONAL SECURITY.

Classified programs remain subject to applicable national-security law. Rules may protect operational details but shall preserve provenance, access logging, inspector-general oversight, retention authority, and periodic review to the maximum extent consistent with national security.

SEC. 41. RULEMAKING.

Within 24 months, DOJ, OMB, NARA, NIST, and the Stewardship Board shall issue coordinated rules on risk tiers, provenance schemas, logging, derived records, residency, AI documentation, correction, deletion, and legacy-system migration.

SEC. 42. PREEMPTION.

This Act establishes a floor and does not preempt stronger State or local protections. A State may not authorize conduct prohibited by Federal law.

SEC. 43. SEVERABILITY.

If any provision or application is held invalid, the remainder and other applications shall not be affected.

SEC. 44. EFFECTIVE DATES.

Rulemaking and inventories begin on enactment; new systems comply within 24 months; existing systems within 48 months; high-risk legacy systems receive priority migration and interim safeguards.

7. Section-by-Section Rationale

Sections	Rationale
1-5	Create the general code, identify federal reach, and define operations broadly enough to avoid device-specific loopholes.
6-10	Establish stewardship identity, lawful entry, provenance, and quality classification. These borrow from the Privacy Act, criminal-history rules, archives practice, and classified markings.
11-18	Govern custody, storage, replication, access, transfer, and contractors. This is where comparative localization and exporter-

	accountability mechanisms are adapted.
19-23	Regulate purpose change, transformation, AI, training, and corroboration. These provisions distinguish observation from inference and prevent model output from becoming self-authenticating government fact.
24-26	Create a real lifespan: maximum retention, periodic review, scoped holds, and graph-aware deletion.
27-30	Create rights triggered by material reliance, avoiding a universal real-time disclosure rule that would compromise investigations.
31-36	Build institutional oversight, security, procurement, and grant implementation.
37-40	Provide calibrated enforcement and preserve emergency and national-security functionality without blanket exemptions.
41-44	Delegate technical standards, preserve stronger state law, phase migration, and protect severability.

8. Constitutional and Administrative-Law Analysis

8.1 Commerce Clause and federal procurement

GISA directly regulates federal agencies, federal contractors, and interstate information services. Provider and contractor obligations are supported by interstate commerce and procurement authority. The legislative record should document nationwide cloud, vendor, and interagency networks.

8.2 Spending Clause and anti-commandeering

State and local agency duties should attach through clear, prospective, program-related grant conditions rather than an unsupported command to administer federal law. Direct federal regulation of private interstate vendors remains distinct from commandeering state legislatures.

8.3 First Amendment

Most provisions regulate conduct, system architecture, government use, and factual commercial disclosures. Restrictions tied to protected activity should be drafted as limits on government investigation, not viewpoint discrimination. Transparency obligations should be factual and reasonably related to preventing deception and enabling oversight.

8.4 Due process and vagueness

Definitions should include objective criteria, risk-tier rules, advisory opinions, safe harbors for good-faith legacy migration, and heightened culpability for damages. High-impact adverse actions receive stronger notice, explanation, and contest rights.

8.5 Records preservation versus deletion

GISA must coexist with the Federal Records Act, FOIA, litigation holds, discovery, Brady obligations, and archival preservation. The solution is not categorical deletion; it is documented authority, separation of archival from operational access, and periodic review.

8.6 Sovereign immunity

The model private action requires legislative-counsel refinement. Prospective relief, federal-agency waivers, contractor liability, individual-capacity remedies where otherwise available, and clear grant conditions are more secure than assuming broad abrogation of state immunity.

9. Research Avenues Tested and Rejected or Limited

Idea	Assessment	Disposition

Hazardous-material analogy	Useful for custody manifests, access tiers, and incident reporting; rhetorically misleading as a central metaphor	Borrow controls, omit label
Universal state-by-state localization	Fragments national systems, reduces resilience, and may trigger federalism/commerce issues	Reject
Citizen-residence “data citizenship”	Ambiguous for travel, mixed datasets, noncitizens, and multi-state events	Reject
Primary jurisdiction and authoritative copy	Administrable and tied to the collecting authority	Adopt
Git-like lineage for every byte	Conceptually strong but disproportionate for low-risk data and difficult for legacy systems	Adopt for material transformations and high-risk systems
Automatic deletion from model weights	Often unverifiable or technically infeasible	Use ex ante training controls, dataset deletion, and model-use restrictions
Treat every AI output as evidence	Overbroad; many outputs are transient aids	Create derived-record status when preserved, shared, or materially relied upon
Real-time notice for every query	Would compromise investigations and overwhelm systems	Trigger notice upon material reliance, with judicial delay

10. Implementation Roadmap

Phase	Timing	Primary work
Foundation	0-12 months	Board, agency inventories, interim preservation of logs, proposed rules, provenance schema pilots
New systems	12-24 months	GISA clauses in procurement; risk tiering; new-system compliance; model inventory
High-risk migration	24-36 months	Tier 4-5 legacy systems, cross-jurisdiction agreements, correction portals, independent audits
General migration	36-48 months	Remaining systems, contractor flow-down, archival/operational separation
Evaluation	48-60 months	Congressional review, metrics, rule revision, technology and federalism assessment

11. Evaluation Metrics

- Percentage of systems with identified steward, authority, risk tier, authoritative copy, and complete storage inventory.
- Percentage of lifecycle operations recorded with complete user, purpose, authority, and recipient fields.
- Number of unauthorized or anomalous accesses and average containment time.
- Number of derived high-impact records used in adverse actions and proportion with documented corroboration.
- Correction requests, substantiation rates, propagation times, and recurrence of corrected errors.
- Volume and purpose of interagency, cross-jurisdiction, and international transfers.
- Retention exceptions and holds older than schedule, with reasons and review status.
- AI training datasets approved, rejected, segregated, and retired.
- Contractor and subprocessor compliance findings, including undisclosed locations or access.

12. Conclusion

The United States does not need to choose between operationally useful government information and civil liberty. It needs a legal architecture that recognizes what digital systems actually do. Information is not merely collected and stored. It is copied, queried, transformed, inferred from, exported, trained upon, and converted into decisions. Each operation changes risk and should change legal responsibility.

GISA's central proposition is that government possession or control creates stewardship. That duty is nondelegable, technology-neutral, and continuous. Provenance, jurisdiction, purpose, transformation, and descendants are part of the legal identity of information. With those concepts, Congress can preserve legitimate investigation while preventing distributed infrastructure and AI from dissolving accountability.

Authorities and Research Notes

Primary legal authorities and official government materials are prioritized. Comparative materials are cited for legislative mechanisms, not as endorsements of any jurisdiction's political system.

1. U.S. CONST. amend. IV.

2. 5 U.S.C. § 552a (Privacy Act of 1974).

3. 44 U.S.C. chs. 21, 29, 31, 33 (Federal Records Act framework).

4. 36 C.F.R. pts. 1220-1239 (Federal records management).

5. 18 U.S.C. §§ 2701-2713 (Stored Communications Act).

6. 15 U.S.C. § 1681 et seq. (Fair Credit Reporting Act).

7. 18 U.S.C. §§ 2721-2725 (Driver's Privacy Protection Act).

8. 28 C.F.R. pt. 20 (Criminal Justice Information Systems).

9. 45 C.F.R. §§ 164.308, 164.312, 164.502, 164.524, 164.526 (HIPAA administrative, technical, use, access, and amendment rules).

10. Executive Order 13,526, Classified National Security Information, 75 Fed. Reg. 707 (Dec. 29, 2009).

11. 32 C.F.R. pt. 2001 (Classified National Security Information).

12. United States v. Jones, 565 U.S. 400 (2012).

13. Riley v. California, 573 U.S. 373 (2014).

14. Carpenter v. United States, 585 U.S. 296 (2018).

15. Chatrie v. United States, No. 25-112 (U.S. June 29, 2026).

16. United States v. Jacobsen, 466 U.S. 109 (1984).

17. Brady v. Maryland, 373 U.S. 83 (1963).

18. Bullcoming v. New Mexico, 564 U.S. 647 (2011) (forensic evidence and testimonial reliability context).

19. Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

20. Reno v. Condon, 528 U.S. 141 (2000).

21. South Dakota v. Dole, 483 U.S. 203 (1987).

22. Murphy v. NCAA, 584 U.S. 453 (2018).

23. National Archives and Records Administration, Universal Electronic Records Management Requirements, https://www.archives.gov/records-mgmt/policy/universalermrequirements.

24. NARA, Metadata Requirements for Permanent Electronic Records (updated Apr. 10, 2025), https://www.archives.gov/records-mgmt/policy/metadata-compiled.

25. NARA Bulletin 2025-01, Metadata Guidance for the Transfer of Classified Electronic Records, https://www.archives.gov/records-mgmt/bulletins/2025/2025-01.

26. FBI, Criminal Justice Information Services Security Policy v5.9.5 (July 9, 2024), https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center/cjis_security_policy_v5-9-5_20240709.pdf.

27. U.S. Department of Justice, Artificial Intelligence and Criminal Justice, Final Report (Dec. 2024), https://www.justice.gov/olp/media/1381796/dl.

28. NIST, Artificial Intelligence Risk Management Framework 1.0, NIST AI 100-1 (2023), https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf.

29. NIST, Artificial Intelligence Risk Management Framework: Generative AI Profile, NIST AI 600-1 (2024), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf.

30. NIST, Privacy Framework 1.0 (2020), https://www.nist.gov/privacy-framework.

31. Directive (EU) 2016/680, arts. 4-5, 7-9, 25, 35-40, 2016 O.J. (L 119) 89, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680.

32. Regulation (EU) 2016/679 (GDPR), arts. 5, 17, 30, 44-50.

33. Brazil, Lei No. 13.709/2018 (LGPD), arts. 5, 15-16, 23-30, 33-36, https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709compilado.htm.

34. Personal Information Protection Law of the People's Republic of China, arts. 38-40, https://en.spp.gov.cn/2021-12/29/c_948419.htm.

35. State Council of China, Regulations on Network Data Security Management (2024), https://english.www.gov.cn/policies/latestreleases/202409/30/content_WS66fab6c8c6d0868f4e8eb720.html.

36. Russian Federal Law No. 242-FZ and Roskomnadzor localization guidance, https://pd.rkn.gov.ru/docs/Obzor_po_lokalizacii.docx.

37. Office of the Australian Information Commissioner, APP 8 - Cross-border Disclosure of Personal Information, https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information.

38. Office of the Privacy Commissioner of Canada, Guidelines for Processing Personal Data Across Borders, https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/.

39. U.S. GAO, Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks of Facial Recognition, GAO-21-518 (2021).

40. U.S. GAO, Facial Recognition Technology: Federal Agencies' Use and Related Privacy Protections, GAO-22-106100 (2022).

41. Federal Trade Commission, Gravy Analytics/Venntel final complaint and order materials, Matter No. 2123035 (2024).

42. Private Infrastructure, Public Power: A Problem Brief (July 19, 2026).

43. Government Data Lifecycle Accountability Act Research Report, version 1 (July 2026).

44. Statute 2 Comparative Data Sovereignty and Lifecycle Research Supplement (July 2026).